

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of:

Ashot Andreyan

Examiner: HA, Leynna A.

Application No.: 10/605,173

Art Unit: 2135

Filed: September 12, 2003

Confirmation No.: 2172

For: KEY EXCHANGE BASED ON DSA  
TYPE CERTIFICATES

Docket No.: PR 1803.01 US

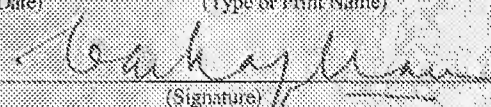
**APPEAL BRIEF**

**Mail Stop APPEAL BRIEF-PATENTS**

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

CERTIFICATE OF ELECTRONIC TRANSMISSION	
I hereby certify that this correspondence is being electronically transmitted to the U.S. Patent and Trademark Office on:	
12.27.2007 (Date)	Bac-Ha Phan (Type or Print Name)
 (Signature)	

Dear Sir:

Applicant submits the following Appeal Brief pursuant to 37 C.F.R. § 41.37 for consideration by the Board of Patent Appeals and Interferences. Please charge any additional fees or credit any overpayment to our deposit Account No. 04-1175.

**TABLE OF CONTENTS**

I.	REAL PARTY IN INTEREST .....	3
II.	RELATED APPEALS AND INTERFERENCES .....	3
III.	STATUS OF CLAIMS.....	3
IV.	STATUS OF AMENDMENTS.....	3
V.	SUMMARY OF CLAIMED SUBJECT MATTER.....	3
VI.	GROUND OF REJECTION TO BE REVIEWED ON APPEAL.....	6
VII.	ARGUMENTS .....	7
A.	Claims 1-35 Are Not Anticipated by Roy (U.S. 6,677,888).....	7
B.	Claims 33-35 Are Not Obvious over Roy and Yeager (US 7,222,187).....	11
VIII.	CONCLUSION .....	14
IX.	CLAIM APPENDIX .....	15
X.	EVIDENCE APPENDIX.....	20
XI.	RELATED PROCEEDINGS APPENDIX.....	20

**I. REAL PARTY IN INTEREST**

The real party in interest is the assignee, Pioneer Research Center USA, Inc.

**II. RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences known to the appellant, the appellant's legal representative, or assignee, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**III. STATUS OF CLAIMS**

Claims 1-35 of the present application are pending. The Applicant hereby appeals the rejection of claims 1-35.

**IV. STATUS OF AMENDMENTS**

On April 17, 2007, Applicant filed a response to an Office Action dated January 17, 2007. The Examiner issued a Final Office Action on July 2, 2007. A proposed amendment was filed on August 29, 2007. The Examiner issued an Advisory Action on September 17, 2007 stating that the proposed amendment would not be entered. Accordingly, no amendment is entered after the final Office Action. On September 28, 2007, the Applicant filed a Notice of Appeal and a Pre-Appeal Brief Review Request in response to the Final Office Action. On September 25, 2007, the Review panel issued the Notice of Panel Decision stating that the application remains under appeal.

**V. SUMMARY OF CLAIMED SUBJECT MATTER**

1. Independent claims 1, 9, 17 and 25:

Independent Claim 1 recites, "A method for generating a shared key comprising:

providing a first certificate from a first peer to a second peer (Figure 5, step 505 and paragraph [0040]), the first certificate including a plurality of first parameters (paragraph [0040],  $g_{dss}$ ,  $p_{dss}$ ), the first peer and second peer (paragraph [0040], Peer A and Peer B) being communicated over a network (paragraph [0003], line 1 and paragraph [0040]; performing a first exponentiation operation (paragraph [0040], symbol  $\wedge$  for exponentiation operation) to generate a first public key (paragraph [0040],  $Y_R$ ) from the second peer (paragraph [0040], Peer B) using at least one parameter of the plurality of first parameters and a first private key from the second peer (Figure 5 (step 510), and paragraph [0040] (parameter  $g_{dss}$  as the at least one parameter

and  $X_R$ , the private key)), wherein the first parameters being digital signature standard parameters (paragraphs [0040 and 42]); providing a second certificate and the first public key from the second peer to the first peer (paragraph [0040], Cert ( $Y_{Bdss}$ , ...), Figure 5 (step 515)), the second certificate comprising a plurality of second parameters; performing a second exponentiation operation (paragraph [0040], " $\wedge$ " as exponentiation operation) to generate a shared secret key (paragraph [0040] ( $Y_{SSK}$ ), Figure 5 (step 520)) for the second peer using at least one parameter from the plurality of first parameters (paragraph [0040],  $g_{dss}$  or  $p_{dss}$ ); performing a third exponentiation operation to generate the shared secret key (Figure 5 (step 525), paragraph [0040] ( $Y_{SSK}$  as shared secret key)) for the first peer (paragraph [0040], Peer A) using the first public key (paragraph [0040] ( $Y_R$ )) from the second peer and a private key from the first peer (paragraph [0040] ( $X_{Adss}$ ))."

Independent claim 9 recites, "An article of manufacture comprising: a machine accessible medium including data that, when accessed by a machine, causes the machine to perform operations comprising: providing a first certificate from a first peer to a second peer (Figure 5, step 505 and paragraph [0040]), the first certificate including a plurality of first parameters (paragraph [0040],  $g_{dss}$ ,  $p_{dss}$ ); performing a first exponentiation operation (paragraph [0040], symbol  $\wedge$  for exponentiation operation) to generate a first public key (paragraph [0040],  $Y_R$ ) from the second peer (paragraph [0040], Peer B) using the plurality of first parameters and the first private key from the second peer (Figure 5 (step 510), and paragraph [0040] (parameter  $g_{dss}$  as the at least one parameter and  $X_R$ , the private key)), wherein the first parameters being digital signature standard parameters (paragraphs [0040 and 42]); providing a second certificate and the first public key from the second peer to the first peer (paragraph [0040], Cert ( $Y_{Bdss}$ , ...), Figure 5 (step 515)), the second certificate comprising a plurality of second parameters; performing a second exponentiation operation (paragraph [0040], " $\wedge$ " as exponentiation operation) to generate a shared secret key (paragraph [0040] ( $Y_{SSK}$ ), Figure 5 (step 520)) for the second peer using at least one parameter from the plurality of first parameters (paragraph [0040],  $g_{dss}$  or  $p_{dss}$ ); performing a third exponentiation operation to generate the shared secret key (Figure 5 (step 525), paragraph [0040] ( $Y_{SSK}$  as shared secret key)) for the first peer (paragraph [0040], Peer A) using the first public key (paragraph [0040] ( $Y_R$ )) from the second peer and a private key from the first peer (paragraph [0040] ( $X_{Adss}$ ))."

Independent claim 17 recites, "A system comprising: a processor; and a memory coupled to the processor, the memory containing program code that, when executed by the

processor, causes the processor to: provide a first certificate from a first peer to a second peer (Figure 5, step 505 and paragraph [0040]), the first certificate including a plurality of first parameters (paragraph [0040],  $g_{dss}$ ,  $p_{dss}$ ), the first peer and second peer (paragraph [0040], Peer A and Peer B) being communicated over a network (paragraph [0003], line 1 and paragraph [0040]; perform a first exponentiation operation (paragraph [0040], symbol  $\wedge$  for exponentiation operation) to generate a first public key (paragraph [0040],  $Y_R$ ) from the second peer (paragraph [0040], Peer B) using the plurality of first parameters and the first private key from the second peer (Figure 5 (step 510), and paragraph [0040] (parameter  $g_{dss}$  as the at least one parameter and  $X_R$ , the private key)), the second parameters being digital signature standard parameters; provide a second certificate and the first public key from the second peer to the first peer (paragraph [0040], Cert ( $Y_{Bdss}$ , ...), Figure 5 (step 515)); the second certificate comprising a plurality of second parameters; perform a second exponentiation operation (paragraph [0040], " $\wedge$ " as exponentiation operation) to generate a shared secret key (paragraph [0040] ( $Y_{SSK}$ ), Figure 5 (step 520)) for the second peer using at least one parameter from the plurality of first parameters (paragraph [0040],  $g_{dss}$  or  $p_{dss}$ ); performing a third exponentiation operation to generate the shared secret key (Figure 5 (step 525), paragraph [0040] ( $Y_{SSK}$  as shared secret key)) for the first peer (paragraph [0040], Peer A) using the first public key (paragraph [0040] ( $Y_R$ )) from the second peer and a private key from the first peer (paragraph [0040] ( $X_{Adss}$ ))."

Independent claim 25 recites: "A method comprising: receiving by a second peer a first certificate of a first peer (paragraph [0040]), including a plurality of first parameters (paragraph [0040],  $g_{dss}$ ,  $p_{dss}$ ), the first peer and second peer (paragraph [0040], Peer A and Peer B) being communicated over a network (paragraph [0003], line 1 and paragraph [0040]; performing a first exponentiation operation (paragraph [0040], symbol  $\wedge$  for exponentiation operation) to generate a first public key (paragraph [0040],  $Y_R$ ) using at least one parameter of the plurality of first parameters and a first private key (Figure 5 (step 510), and paragraph [0040] (parameter  $g_{dss}$  as the at least one parameter and  $X_R$ , the private key)), the second parameters being digital signature standard parameters (paragraphs [0040 and 42]); receiving a second certificate and the first public key (paragraph [0040], Cert ( $Y_{Bdss}$ , ...)), the second certificate including a plurality of second parameters; performing a second exponentiation operation (paragraph [0040], " $\wedge$ " as exponentiation operation) to generate a first shared secret key (paragraph [0040] ( $Y_{SSK}$ ), Figure 5 (step 520)) using at least one parameter from the plurality of first parameters (paragraph [0040],  $g_{dss}$  or  $p_{dss}$ ); performing a third exponentiation operation to generate a second shared

secret key (Figure 5 (step 525), paragraph [0040] ( $Y_{SSK}$  as shared secret key)) using the first public key (paragraph [0040] ( $Y_R$ )) and a private key.”

2. Dependent claims 2-8, 10-16, 18-24 and 26-35:

Dependent claims 2, 10, 18, and 26, recite in essence, “the first certificate is a DSA type certificate; paragraphs [0039] and [0042].”

Dependent claims 3, 11, 19, and 27, recite in essence, “The first and second parameters comprise a prime number  $p_{dss}$ , a prime number  $q_{dss}$ , a generator  $g_{dss}$ , and a public key for the first and second peer, respectively (parameters shown in paragraph [0040]).”

Dependent claims 4, 12, 20, and 28, recite in essence, “the first exponentiation operation to generate the first public key ( $Y_R$ ), (exponentiation operation (1) as shown in paragraph [0040]).”

Dependent claims 5, 13, 21, and 29, recite in essence, “the second exponentiation operation to generate a shared secret key  $Y_{SSK}$  for the second peer (exponentiation operation (2) as shown in paragraph [0040]).”

Dependent claims 6, 14, 22, and 30, recite in essence, “the exponentiation operation of  $Y_{Adss}$  wherein  $Y_{Adss} = g_{dss} ^ X_{Adss} \text{ mod } p_{dss}$ .”

Dependent claims 7, 15, 23, and 31, recite in essence, “the third exponentiation operation to generate a share secret key ( $Y_{SSK}$ ) for the first peer (exponentiation operation (3) as shown in paragraph [0040]).”

Dependent claims 8, 16, 24, and 32, recite in essence, “the first and second certificates are sent via a wireless network.”

Dependent claims 33, 34, and 35, recite in essence, “the wireless network is a Bluetooth network”

VI. GROUND OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-32 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,677,888 issued to Roy (“Roy”).
2. Claims 33-35 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Roy in view of U. S. Patent No. 7,222,187 issued to Yeager, et al. (“Yeager”).

## VII. ARGUMENTS

The Examiner rejected claims 1-35 under 35 U.S.C. §102(e) as being anticipated by Roy; claims 33-35 under 35 U.S.C. §103(a) as being unpatentable over Roy in view of Yeager. Applicant respectfully traverses the rejections and submits that the Examiner has not met the burden of establishing a prima facie case of anticipation and obviousness.

### A. Claims 1-35 Are Not Anticipated by Roy.

Roy discloses a secure Aircraft Addressing and Reporting System (ACARS) solution for protecting the aeronautical information transfer end-to-end over the ACARS data link using standard-based, cryptographic techniques (Col. 3, lines 5-8). Roy discloses a solution to encrypt ACARS protocol header. It also defines protocol to derive secret keys. However, in contrast to the present invention, its secret key derivation is based on random number generated by ground SAM. In the present invention, the secret key derivation is based on using DSA type of digital certificate domain parameters (i.e.,  $p_{dss}$ ,  $q_{dss}$ ,  $g_{dss}$ ). By using the domain parameters, the exponential operations to generate shared secret key is only 3, while in Diffie-Hellman (DH) key exchange, 4 exponential operations is needed.

Roy discloses that on receipt of a request message, the ground SAM would obtain a certificate of the aircraft and the latest of CRL from a certificate depository (CD).... It then verifies the signature at  $s_u$ , using ECDSA algorithm (Col. 10, lines 58-64). Roy also discloses that according to ECDSA signature and verification operations, to generate a key pair, an entity first selects an elliptic curve  $E$  and a point  $G$  on  $E$ . The entity then selects a private key  $d$ , which is an integer picked at random, and computes the public key  $dG$ . To sign a message  $M$ , the SAM processes  $M$  with a known hash function called SHA-1,...Then the entity selects an integer  $k$  at random, ... When the receiving SAM process wants to verify the signature  $(r, s)$  on the message  $M$  it retrieves the public key  $Q=dG$  of the sending... The signature is genuine if the two values are equal (Col. 9, lines 41-60). The certificate authority (CA), which is a trusted entity that issues the asymmetric cryptographic keys, the public key certificates, and the Certificate Revocation Lists (CRL)... the domain parameters and the key size determine the cryptographic strength (Col. 10, lines 27-32). Roy discloses that to establish a secret session key, the airborne SAM creates an Initialization\_request message. The airborne SAM signs this message and sends this message with the signature to the ground SAM. (Col. 10, lines 48-52). Roy also discloses the elliptic curve Diffie-Hellman (DH) key agreement scheme operation that shown in Col. 10 (lines 1-9).

Regarding Col. 10, lines 58-64 of Roy, applicant is well aware that the certificate obtained from the aircraft can be considered as the first certificate, as well as, the first certificate can be obtained from any protocol. The certificate can be part of any network protocol, for example, IKE (Internet Key Exchange) protocol, or SSL (Secured Socket Layer) protocol... Also, applicant is also aware that all protocols exchange certificates during a hand shake and that certificate is digitally signed. However, the present invention is not about issuing a certificate as disclosed in Roy but to utilize parameters from a certificate to generate a secret key by using only 3 exponential operations.

Regarding Col. 9, lines 41-60 of Roy, these lines talk about generating ECC certificate. Unlike Roy, in the present invention, that certificate is assumed to have been issued by CA already. Each peer just uses DSA parameters from already issued certificates. This operation calculates only new public/private key by using DSA parameters from the certificate. Then the new generated public key is sent to the first peer, along with the second peer certificate where part of protocol for session key derivation is disclosed in paragraphs 39 to 40.

Regarding Col. 10, lines 27-32 of Roy, it is true that each system can choose to use some CA and that key sizes can be defined as well. However, the present invention is not about defining and enrolling certificates. The operations in the present invention assume that certificates are already issued by CA and both peers have DSA type of certificates and that they are valid.

Regarding Col. 10, lines 48-52 of Roy, these lines describe protocol between an aircraft and ground SAM. The present invention does not claim protocol but a key exchange method or a key establishment method, which can be used in any protocol (including those protocols disclosed in Roy).

Regarding Col. 10, lines 1-9 of Roy, these lines discuss how Diffie-Helman (DH) shared secret key is established on ECC. In contrast to the present invention, where DSA parameters are used; these DSA parameters are not the same as DH parameters. Furthermore, the first peer does not generate DH public/private key but it just sends a certificate. The second peer generates one time public/private key pair by using domain parameters (i.e., DSA parameters), which are not the same as DH parameters. In summary, classic DH key exchange requires 4 exponentiation operations (2 operations on each side): one for generating DH public/private key and one for generating shared secret key on each side. The claimed invention generates the shared secret key by 3 exponentiation operations only by using DSA parameters.



Roy does not disclose, either implicitly or explicitly generating a secret key by 3 exponentiation operations using DSA parameters. In other words, nowhere in Roy that discloses using DSA parameters to generate a secret key by only 3 exponential operations.

In summary, there are several clear errors in the Examiner's rejections and arguments.

1) Roy does not disclose the step of "performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer, wherein the first parameters being digital signature standard parameters", the Examiner cited Roy (col. 9, lines 44-60). The Examiner stated, "Roy discloses generating by computing the public key which selects a private key and to sign a message with a known hash function (SHA-1) thereby obtaining a digital fingerprint of the message. The hash that obtains the digital fingerprint is claimed to the 1st parameters being signature standard parameters." There is nothing in Roy that discloses using a DSS parameter to generate a public key. Roy only discloses, "... To sign a message M, the SAM processes M with a known hash function called SHA-1, thereby obtaining a digital fingerprint SHA-1(M) of the message ..." Roy discloses the generating of ECC certificate when the present invention assumes that the certificate has already issued by CA.

2) Roy does not disclose the step of "providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters", the Examiner cited Roy (col. 10, lines 27-32). The Examiner stated, "Roy discloses the CA issues the public key certificates with domain parameters and the key size to determine the cryptographic strength as the claimed provided the 2nd certificate and public key with 2nd parameters." This may be true. Each system can choose to use some CA and key sizes can be defined as well. However, defining and enrolling certificates are out of the scope of the claimed invention. As stated before, the claimed invention assumes that certificates are already issued by CA and both peers have DSA type of certificates and that they are valid. Furthermore, the first public key provided from the second peer to the first peer was calculated using a DSS parameter. There is nothing in Roy that discloses the public key was generated using a DSS parameter.

3) Roy does not disclose the step of "performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters", the Examiner cited Roy (col. 10, lines 48-52). The Examiner stated, "Roy discusses a secret session key is established in a request message that sends the message with the signature as the claimed shared secret key using a parameter from

the first parameters. The parameter from the first parameters is referring to signature standard parameters as claimed above.” Roy discloses protocol between aircraft and ground SAM. The present invention is not a protocol. It is a key exchange method, key establishment method, which can be used in any protocol as well as the protocol disclosed in Roy.

4) Roy does not disclose the step of “performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer”, the Examiner cited Roy (col. 10, lines 1-9). Roy discloses an elliptic curve Diffie-Hellman key agreement scheme that operates as follows: when two entities (U and V) want to establish a shared secret key, they exchange their public keys  $duG$  and  $dvG$  where  $du$  and  $dv$  are private keys of the corresponding entities U and V. Then both entities compute a share secret... Roy discloses how Diffie-Hellman shared secret is established on ECC. The mechanism in the claimed invention is different. First of all, it uses DSA parameters, which are not the same as DH parameters. Secondly, the first peer in the claimed invention does not generate DH public/private key. It just sends its certificate. The second peer in the claimed invention generates public/private key pair by using DSA parameters from the certificate sent from the first peer. Furthermore, classic DH key exchange (which is disclosed in Roy) requires 4 exponentiation operations (2 on each side). Each side uses 2 exponentiation operations; one for generating DH public/private key and one for generating shared secret key. The claimed invention can generate a shared secret key by a total of 3 exponentiation operations only.

To anticipate a claim, the reference must teach every element of the claim. “A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” Vergegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). “The identical invention must be shown in as complete detail as is contained in the...claim.” Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989). Since the Examiner failed to show that Roy teaches or discloses any one of the above elements, the rejection under 35 U.S.C. §102 is improper.

Therefore, Applicant believes that independent claims 1, 9, 17 and 25 and their respective dependent claims are distinguishable over the cited prior art references.

**B. Claims 33-35 Are Not Obvious over Roy and Yeager.**

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *MPEP* §2143, p. 2100-126 to 2100-130 (8th Ed., Rev. 5, May 2006). Applicant respectfully contends that there is no suggestion or motivation to combine their teachings, and thus no *prima facie* case of obviousness has been established.

Furthermore, the Supreme Court in *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966), stated: “Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.” *MPEP* 2141. In *KSR International Co. vs. Teleflex, Inc.*, 127 S.Ct. 1727 (2007) (Kennedy, J.), the Court explained that “[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” The Court further required that an explicit analysis for this reason must be made. “[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR* 127 S.Ct. at 1741, quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). In the instant case, Applicant respectfully submits that there are significant differences between the cited references and the claimed invention and there is no apparent reason to combine the known elements in the manner as claimed, and thus no *prima facie* case of obviousness has been established.

Roy is discussed above. Yeager discloses that in order to interact with other peers; the peer needs to be connected to some kind of network, such as IP, Bluetooth, or Havi, among others (Col. 27, lines 29-35). Yeager further discloses that the peer-to-peer platform may be independent of transport protocols. For example, the peer-to-peer platform may be implemented on top of TCP/IP, HTTP, Bluetooth, Home-PNA, and other protocols (Col. 33, lines 21-25). Yeager, however, does not disclose generating a secret key by 3 exponentiation operations using DSA parameters.

As discussed above, Roy or Yeager does not disclose or suggest elements (1) through (4). Accordingly, a combination of Roy or Yeager in rejecting claims 33-35, which depend on claims 1, 17, and 25, respectively, is improper.

There is no motivation to combine Roy and Yeager because none of them addresses the problem of generating a secret key by exponentiation operations using DSA parameters in a Bluetooth network. Roy or Yeager, read as a whole, does not suggest the desirability of generating a secret key by 3 exponentiation operations using DSA parameters let alone over a Bluetooth network. For the above reasons, the rejection under 35 U.S.C. §103(a) is improperly made.

The Examiner failed to establish a prima facie case of obviousness and failed to show there is teaching, suggestion, or motivation to combine the references. When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to: (A) The claimed invention must be considered as a whole; (B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination; (C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention; and (D) Reasonable expectation of success is the standard with which obviousness is determined. Hodosh v. Block Drug Co., Inc., 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986). "When determining the patentability of a claimed invention which combined two known elements, 'the question is whether there is something in the prior art as a whole suggest the desirability, and thus the obviousness, of making the combination.'" In re Beattie, 974 F.2d 1309, 1312 (Fed. Cir. 1992), 24 USPQ2d 1040; Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co., 730 F.2d 1452, 1462, 221 USPQ (BNA) 481, 488 (Fed. Cir. 1984). To defeat patentability based on obviousness, the suggestion to make the new product having the claimed characteristics must come from the prior art, not from the hindsight knowledge of the invention. Interconnect Planning Corp. v. Feil, 744 F.2d 1132, 1143, 227 USPQ (BNA) 543, 551 (Fed. Cir. 1985). To prevent the use of hindsight based on the invention to defeat patentability of the invention, this court requires the Examiner to show a motivation to combine the references that create the case of obviousness. In other words, the Examiner must show reasons that a skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the prior elements from the cited prior references for combination in the manner claimed. In re Rouffet, 149 F.3d 1350 (Fed. Cir. 1996), 47 USPQ 2d (BNA) 1453. "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or implicitly

suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 227 USPQ 972, 973. (Bd.Pat.App.&Inter. 1985). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Furthermore, although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." In re Mills 916 F.2d at 682, 16 USPQ2d at 1432; In re Fritch, 972 F.2d 1260 (Fed. Cir. 1992), 23 USPQ2d 1780.

Moreover, the Examiner failed to establish the factual inquires in the three-pronged test as required by the *Graham* factual inquires. There are significant differences between the cited references and the claimed invention as discussed above. Furthermore, the Examiner has not made an explicit analysis on the apparent reason to combine the known elements in the fashion in the claimed invention. Accordingly, there is no apparent reason to combine the teachings of Roy and Yeager.

In the present invention, the cited references do not expressly or implicitly suggest any of the above elements. In addition, the Examiner failed to present a convincing line of reasoning as to why a combination of Roy and Yeager is obvious.

Therefore, Applicant believes that independent claims 1, 9, 17 and 25, and their respective dependent claims are distinguishable over the cited prior art references.

**VIII. CONCLUSION**

Applicant respectfully requests that the Board enter a decision overturning the Examiner's rejection of all pending claims, and holding that the claims satisfy the requirements of 35 U.S.C. §102(e) and 35 U.S.C. §103(a).

Respectfully submitted,  
PIONEER NORTH AMERICA, INC.

Dated: \_\_\_\_\_

12/26/07

Caroline T. Do

Caroline T. Do  
Reg. No. 47,529

PIONEER NORTH AMERICA, INC.  
INTELLECTUAL PROPERTY DEPARTMENT  
2265 E. 220<sup>th</sup> Street  
Long Beach, CA 90810  
(310) 952-3300

## IX. CLAIM APPENDIX

The claims of the present application which are involved in this appeal are as follows:

1. (Previously amended) A method for generating a shared key comprising:
  - providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters, the first peer and second peer being communicated over a network;
  - performing a first exponentiation operation to generate a first public key from the second peer using at least one parameter of the plurality of first parameters and a first private key from the second peer, wherein the first parameters being digital signature standard parameters;
  - providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;
  - performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;
  - performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.
2. (Original) The method according to claim 1 wherein the first certificate is a DSA type certificate.
3. (Original) The method according to claim 2 wherein the first and second parameters comprise a prime number  $p_{dss}$ , a prime number  $q_{dss}$ , a generator  $g_{dss}$  and a public key for the first and second peers, respectively.
4. (Original) The method according to claim 3 wherein the first exponentiation operation to generate the first public key is  $Y_R = g_{dss}^{X_R} \bmod p_{dss}$  where  $X_R$  is a one-time private key from the second peer.
5. (Original) The method according to claim 4 wherein the second exponentiation operation to generate the shared secret key for the second peer is  $Y_{SSK} = Y_{Adss}^{X_R} \bmod p_{dss}$  where  $Y_{Adss}$  is a DSS public key from certificate of peer A.
6. (Original) The method according to claim 5 wherein  $Y_{Adss} = g_{dss}^{X_{Adss}} \bmod p_{dss}$  where  $X_{Adss}$  is a DSS private key from certificate of peer A.

7. (Original) The method according to claim 5 wherein the third exponentiation operation to generate the shared secret key for the first peer is  $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$  where  $X_{Adss}$  is a DSS private key from certificate of peer A.
8. (Original) The method according to claim 1 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.
9. (Previously amended) An article of manufacture comprising:
  - a machine accessible medium including data that, when accessed by a machine, causes the machine to perform operations comprising:
    - providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters;
    - performing a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer, wherein the first parameters being digital signature standard parameters;
    - providing a second certificate and the first public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;
    - performing a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;
    - performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.
10. (Original) The article of manufacture according to claim 9 wherein the first certificate is a DSA type certificate.
11. (Original) The article of manufacture according to claim 10 wherein the first and second parameters comprise a prime number  $p_{dss}$ , a prime number  $q_{dss}$ , a generator  $g_{dss}$  and a public key for the first and second peers, respectively.
12. (Original) The article of manufacture according to claim 11 wherein the first exponentiation operation to generate the first public key is  $Y_R = g_{dss} \wedge X_R \bmod p_{dss}$  where  $X_R$  is a one-time private key from the second peer.



13. (Original) The article of manufacture according to claim 12 wherein the second exponentiation operation to generate the shared secret key for the second peer is  $Y_{SSK} = Y_{Adss} \wedge X_R \bmod p_{dss}$  where  $Y_{Adss}$  is a DSS public key from certificate of peer A.

14. (Original) The article of manufacture according to claim 13 wherein  $Y_{Adss} = g_{dss} \wedge X_{Adss} \bmod p_{dss}$  where  $X_{Adss}$  is a DSS private key from certificate of peer A.

15. (Original) The article of manufacture according to claim 13 wherein the third exponentiation operation to generate the shared secret key for the first peer is  $Y_{SSK} = Y_R \wedge X_{Adss} \bmod p_{dss}$  where  $X_{Adss}$  is a DSS private key from certificate of peer A.

16. (Original) The article of manufacture according to claim 9 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

17. (Previously amended) A system comprising:

a processor; and

a memory coupled to the processor, the memory containing program code that, when executed by the processor, causes the processor to:

provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters, the first peer and second peer being communicated over a network;

perform a first exponentiation operation to generate a first public key from the second peer using the plurality of first parameters and the first private key from the second peer; the second parameters being digital signature standard parameters;

provide a second certificate and the first public key from the second peer to the first peer; the second certificate comprising a plurality of second parameters;

perform a second exponentiation operation to generate a shared secret key for the second peer using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate the shared secret key for the first peer using the first public key from the second peer and a private key from the first peer.

18. (Original) The system according to claim 17 wherein the first certificate is a DSA type certificate.

19. (Original) The system according to claim 18 wherein the first and second parameters comprise a prime number  $p_{dss}$ , a prime number  $q_{dss}$ , a generator  $g_{dss}$  and a public key for the first and second peers, respectively.

20. (Original) The system according to claim 19 wherein the first exponentiation operation to generate the first public key is  $Y_R = g_{dss}^{X_R} \bmod p_{dss}$  where  $X_R$  is a one-time private key from the second peer.

21. (Original) The system according to claim 20 wherein the second exponentiation operation to generate the shared secret key for the second peer is  $Y_{SSK} = Y_{Adss}^{X_R} \bmod p_{dss}$  where  $Y_{Adss}$  is a DSS public key from certificate of peer A.

22. (Original) The system according to claim 21 wherein  $Y_{Adss} = g_{dss}^{X_{Adss}}$  where  $X_{Adss}$  is a DSS private key from certificate of peer A.

23. (Original) The system according to claim 21 wherein the third exponentiation operation to generate the shared secret key for the first peer is  $Y_{SSK} = Y_R^{X_{Adss}} \bmod p_{dss}$  where  $X_{Adss}$  is a DSS private key from certificate of peer A.

24. (Original) The system according to claim 17 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

25. (Previously amended) A method comprising:

receiving by a second peer a first certificate of a first peer including a plurality first parameters, the first peer and second peer being communicated over a network;

performing a first exponentiation operation to generate a first public key using at least one parameter of the plurality of first parameters and a first private key; the second parameters being digital signature standard parameters;

receiving a second certificate and the first public key, the second certificate including a plurality of second parameters;

performing a second exponentiation operation to generate a first shared secret key using at least one parameter from the plurality of first parameters;

performing a third exponentiation operation to generate a second shared secret key using the first public key and a private key.

26. (Original) The method according to claim 25 wherein the first certificate is a DSA type certificate.
27. (Original) The method according to claim 26 wherein the first and second parameters each comprises a prime number  $p_{dss}$ , a prime number  $q_{dss}$ , a generator  $g_{dss}$  and a public key.
28. (Original) The method according to claim 27 wherein the first exponentiation operation to generate the first public key is  $Y_R = g_{dss}^{X_R} \bmod p_{dss}$  where  $X_R$  is a one-time private key.
29. (Original) The method according to claim 28 wherein the second exponentiation operation to generate the first shared secret key for the second peer is  $Y_{SSK} = Y_{Adss}^{X_R} \bmod p_{dss}$  where  $Y_{Adss}$  is a DSS public key.
30. (Original) The method according to claim 29 wherein  $Y_{Adss} = g_{dss}^{X_{Adss}} \bmod p_{dss}$  where  $X_{Adss}$  is a DSS private key.
31. (Original) The method according to claim 29 wherein the third exponentiation operation to generate a second shared secret key is  $Y_{SSK} = Y_R^{X_{Adss}} \bmod p_{dss}$  where  $X_{Adss}$  is a DSS private key.
32. (Original) The method according to claim 25 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.
33. (Previously presented) The method according to claim 1 wherein the network be one of a wireless network and a Bluetooth network.
34. (Previously presented) The system according to claim 17 wherein the network be one of a wireless network and a Bluetooth network.
35. (Previously presented) The method according to claim 24 wherein the network be one of a wireless network and a Bluetooth network.

**X. EVIDENCE APPENDIX**

None

**XI. RELATED PROCEEDINGS APPENDIX**

None